DOI: 10.5748/20CONTECSI/PSE/SEC/7325

eLocator: e207325

MEDIDAS PREVENTIVAS DE SEGURANÇA CIBERNÉTICA PARA USUÁRIOS: UMA REVISÃO SISTEMÁTICA

Wellington Sousa Aguiar – https://orcid.org/0000-0003-0677-5782
Centro Universitário Estácio Do Ceará Universidade Federal Do Ceará - Ufc

Gabriel Anderson Da Silva Ibiapina – https://orcid.org/0009-0005-1547-5337
Centro Universitário Estácio Do Ceará

Paulo Ernesto Vasconcelos Crisóstomo Júnior – https://orcid.org/0009-0007-9289-7351
Centro Universitário Estácio Do Ceará

Cássio Pinheiro Oliveira – https://orcid.org/0000-0001-8004-8087
Centro Universitário Estácio Do Ceará

CYBERSECURITY PREVENTIVE MEASURES FOR USERS: A SYSTEMATIC REVIEW

ABSTRACT

Cybercrimes grow year by year, affecting both companies and lay people who use the internet daily. The increased integration of forms of payment in the virtual environment and the use of social networks awaken opportunities for criminals to act and exploit vulnerabilities. The objective of this work is to conduct a systematic review on the subject of cybersecurity in the post-pandemic period, in order to point out patterns in attacks and describe ways to avoid them. The methodology used was a systematic review and bibliographic review in articles and websites about the most common types of attacks carried out during and after the 2019 pandemic and the documented damages. In the study it was possible to observe an increase of scams using social engineering concepts in registered attacks on lay people and a growth of attacks on private companies using Ransomware. The work finally presents some personal protection tools, such as OpenBSD and Virustotal. Finally, looking at the personal security landscape, we can conclude that the evolution of social engineering threats has become sophisticated enough to fool a significant portion of the general population. In the context of enterprise security it was possible to see a preference for Ransomware attacks, given the tendency of companies to concentrate critical user and market data, which make attacks more effective for obtaining rescues.ile.

Keywords: Malware; Ransomware; Social engineering; Information security.

MEDIDAS PREVENTIVAS DE SEGURANÇA CIBERNÉTICA PARA USUÁRIOS: UMA REVISÃO SISTEMÁTICA

RESUMO

Os crimes cibernéticos crescem ano a no, afetando tanto as empresas quanto as pessoas leigas que utilizam a internet diariamente. O aumento da integração de formas de pagamento no meio virtual e o uso de redes sociais despertam nos criminosos oportunidades de atuação e exploração de vulnerabilidades. O objetivo deste trabalho é realizar uma revisão sistemática sobre o tema segurança cibernética no período pós pandemia, a fim de apontar padrões nos ataques e descrever formas de evitá-los. A metodologia utilizada foi a revisão sistemática e revisão bibliográfica em artigos e sites a respeito dos tipos mais comuns de ataques realizados durante e após a pandemia de 2019 e dos danos documentados. No estudo foi possível observar um aumento de golpes utilizando conceitos de engenharia social em ataques registrados a pessoas leigas e um crescimento de registros de ataques a empresas privadas utilizando Ransomware. O trabalho por fim apresenta algumas ferramentas de proteção pessoal, como OpenBSD e Virustotal. Finalmente, observando o panorama de segurança pessoal, podemos concluir que a evolução das ameaças de engenharia social se tornou sofisticada o suficiente para enganar uma parcela significativa da população em geral. No contexto de segurança empresarial pôde-se constatar uma preferência a ataques de Ransomware, dado a tendência das empresas concentrarem dados críticos de usuários e mercado, que tornam os ataques mais eficazes para obtenção de resgates.

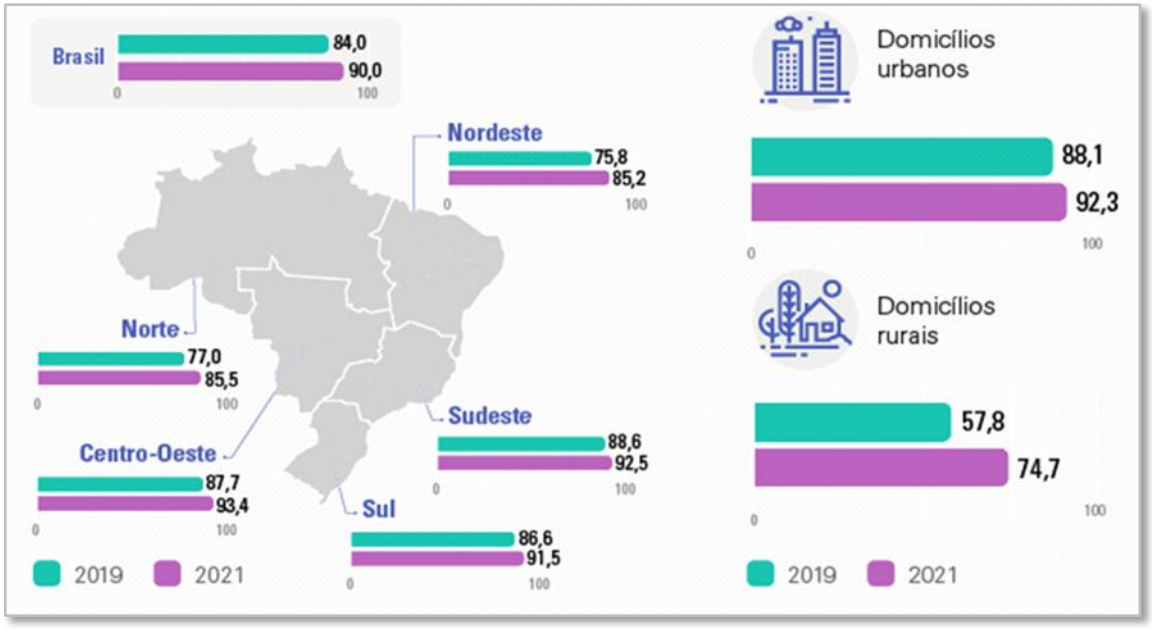
Palavras-chave: Malware; Ransomware; Engenharia social; Segurança da informação.

INTRODUÇÃO

Com o avanço, barateamento e eventual popularização dos sistemas eletrônicos, e a popularização da internet, surgiram muitas facilidades para o nosso dia a dia, especialmente quando se trata de pagamento virtual e entretenimento.

O IBGE afirmou que em 2021, o acesso à internet abrangia 90% dos domicílios do país e que 60% dos idosos já acessam a internet, com ênfase do aumento de acesso via aparelho celular, conforme Figura 1 abaixo.

Figura 1 - Panorama do uso da internet no Brasil.



Fonte: Tecnologia da Informação e Comunicação – IBGE, 2021.

Com as adversidades econômicas e sociais consequentes da pandemia houve uma crescente migração de comércio físico para digital (e-commerce), como aponta um estudo da Mastercard realizado em 2021, que constata um aumento significativo de pequenas e médias empresas que migraram para o comércio eletrônico comparado com a quantidade registrada em 2019, apontando uma nova tendência a empresas se estabelecerem digitalmente.

E como consequência essas mudanças tendem a popularizar o pagamento digital concentrando transações em meio virtual através de serviços como Pix, que de acordo com uma análise realizada pelo Banco central do Brasil, entre outubro de 2021 e setembro de 2023 houve um aumento de 41 Milhões pessoas que já fizeram Pix,

Se torna cada vez mais evidente ao longo dos anos que a internet se tornou um espaço em comum na sociedade no dia a dia, logo, com a constante concentração de transações no contexto virtual, é só questão de tempo para golpistas tentarem a adaptar e criar novos golpes para se adequar ao meio digital.

Sobre o crescimento de golpes e fraudes no meio digital, uma pesquisa da G1 realizada em 2022, aponta o seguinte:

> "Um levantamento da Transunion, empresa global de informações e soluções. mostra que **as tentativas de fraude digital no país cresceram 20% no segundo trimestre deste ano em comparação ao mesmo período de 2021** – 27% das pessoas entrevistadas na pesquisa indicaram que já foram alvo de fraude online nos últimos três meses." (G1,2022)

Com um número cada vez maior de usuários utilizando o mobile e cada vez mais empresas adotando estratégias para esses dispositivos, é normal que os criminosos também voltem seus esforços para os smartphones. Em meio a essa migração, técnicas fraudulentas que só eram possíveis de serem aplicadas em dispositivos via Web são continuamente adaptadas para o mobile. Um exemplo é o RAT, malware que permite ao criminoso ter acesso remoto ao computador da vítima e que agora tem um ataque parecido no celular, conhecido como "golpe da mão fantasma".

De acordo com Indicador de Tentativas de Fraude da Serasa Experian, os brasileiros foram submetidos a quase 4 milhões de tentativas de fraude de identidade em 2022; resultando em uma vítima a cada 9 segundos. São Paulo é o estado que mais recebeu tentativas de fraude de identidade em todo o país com mais de um milhão de ataques registrados. Metade das tentativas de fraude ocorridas no Brasil em 2022 se concentraram em apenas três estados: São Paulo (31%); Rio de Janeiro (11%) e Minas Gerais (9%).

Diante desse cenário crítico, a conscientização em segurança da informação surge como uma medida fundamental para enfrentar o cibercrime no Brasil. A falta de conhecimento sobre os riscos e sobre as boas práticas de segurança contribui para a vulnerabilidade tanto de pessoas quanto de empresas.

A segurança da informação consiste numa série de ações que tem como objetivo registrar, identificar e combater as ameaças que possam surgir em diferentes sistemas. As ameaças é tudo aquilo que pode comprometer a integridade, a confidencialidade e a disponibilidade das informações de uma empresa. Para isso, são implementadas boas práticas e políticas visando controlar os riscos e evitar qualquer tipo de ameaça, essas práticas são conhecidas como os cinco pilares da Segurança da Informação e se dividem em: Integridade, Confidencialidade, Disponibilidade, Autenticidade e Legalidade.

Integridade está relacionada com a necessidade de preservar os dados, ou seja, impedir que o conteúdo deles seja alterado, danificado ou corrompido.

Confidencialidade é uma forma de restringir quem terá acesso aos dados, ou seja, somente pessoas autorizadas deverão acessar as informações. Normalmente é criada uma hierarquia para os dados e quanto mais sensível for a informação para a empresa, menos pessoas poderão acessá-las.

Disponibilidade é a garantia de que a informação estará ativa para ser acessada pelas pessoas autorizadas quantas vezes for necessário, não importando hora e nem dia.

Autenticidade é a forma de prever que os dados são legítimos, verdadeiros e que não foram modificados por pessoas não autorizadas.

Legalidade garante que todos os procedimentos relacionados à Segurança da Informação precisam estar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo que a empresa atue dentro do que prevê a legislação vigente.

Em 27 de maio de 2021, foi sancionado no Brasil a Lei Nº 14.155 que alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informática, furto e estelionato cometidos de forma

eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

Conforme a nova redação do Código, o crime de invasão de dispositivos de informática passará a ser punido com reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. Antes, a pena aplicável era de detenção de três meses a um ano e multa.

A penalidade vale para aquele que invadir um dispositivo a fim de obter, adulterar ou destruir dados ou informações sem autorização do dono, ou ainda instalar vulnerabilidades para obter vantagem ilícita.

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº. 13.709/18) estabelece regras para uso, coleta, armazenamento e compartilhamento de dados dos usuários por empresas privadas e públicas. O objetivo principal é garantir maior segurança, privacidade e transparência no uso de informações pessoais.

A LGPD se aplica a qualquer pessoa física ou jurídica que realize atividades de Tratamento de Dados Pessoais (em meio físico ou virtual) em território brasileiro, ofereça bens ou serviços para Titulares localizados no Brasil ou tenha coletado os Dados Pessoais no Brasil.

A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes. Esclarece ainda que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação. Além disso, a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. A lei autoriza também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos.

Os principais tipos de cibercriminosos são:

Os hackers: pessoas com habilidades avançadas em computação que usam seus conhecimentos para invadir espaços digitais restritos, como redes, servidores, dispositivos pessoais, contas on-line e infraestrutura de nuvem (FortiNET, 2023).

Os crackers: também possuem grande conhecimento em códigos, computadores, informática, hardware e software. Entretanto, eles utilizam todo o conhecimento para realizar alguma ação maléfica em benefício próprio ou para prejudicar outras empresas e pessoas(FortiNET, 2023).

Script Kiddies / Lammers: indivíduos que usam ferramentas de hacking pré-fabricadas para realizar ataques cibernéticos, geralmente sem muito conhecimento técnico.

Spammers: pessoas ou empresas que enviam spam em massa. Eles podem ser motivados por razões comerciais, políticas ou outras.

Scammers: indivíduos ou grupos que realizam scams. Eles podem usar várias técnicas de engenharia social e falsificação de identidade para enganar as pessoas e obter informações valiosas(FortiNET, 2023).

WhistleBlowers: pessoas inseridas em uma empresa e que aproveitam esse acesso livre aos sistemas para vazar informações que podem ser preocupantes. Elas tendem a querer vingança ou até conseguir emprego em outras corporações, por meio da venda de segredos comerciais.

Hacktivistas: são hackers que usam suas habilidades para apoiar causas políticas ou sociais. Eles podem realizar ataques DDoS em sites de empresas ou governos que consideram injustos ou realizar ações para expor informações confidenciais.

Ciberterroristas: São considerados os mais perigosos, possuem repertório amplo de habilidades e objetivos. Em geral, sua intenção é espalhar medo, caos, terror e violência, justificando seus atos com religião ou política.

Os principais tipos de ataques são:

Malware: "software mal-intencionado", ele infecta um computador e altera a forma como ele funciona, destrói dados e pode espionar o tráfego de rede ou do usuário à medida que ele passa (DIO.ME, 2023).

Spams: é o envio de e-mails em massa não solicitados, geralmente para fins de marketing ou propaganda. O spam pode ser enviado por pessoas físicas ou empresas.

Scams: golpes cibernéticos que visam enganar as pessoas para que forneçam informações pessoais, financeiras ou outras informações valiosas. Os scams são geralmente realizados por meio de engenharia social e podem incluir falsos e-mails de phishing, sites fraudulentos e outras táticas.

Vírus: é um programa malicioso que se espalha por meio da inserção de cópias de si mesmo em outros programas executáveis ou arquivos de dados. O objetivo principal dos vírus é danificar ou interromper o funcionamento normal dos sistemas infectados.

Keyloggers: programas maliciosos que são usados para capturar as teclas digitadas em um dispositivo. Eles são frequentemente usados por criminosos cibernéticos para roubar senhas e informações confidenciais.

Trojans: programas maliciosos que se disfarçam como software legítimo e são instalados pelos usuários sem o conhecimento de que eles estão infectando seus sistemas. Os trojans podem ser usados para roubar informações pessoais, como senhas ou dados bancários, ou para permitir que hackers acessem o sistema infectado remotamente (DIO.ME, 2023).

A lista é longa, podemos citar ainda: Backdoors, Exloits, Rootkits, Spywares, Worms, Adwares, Bots, Ransonware, Ataque DoS e DdoS, Ataques MITM, Phishing, Whale Pishing, SpearPhishing, Smishing, Vishing, Ataques por senha, entre outros.

Então é crucial que haja uma conscientização social referente a cibersegurança, para que pessoas que usam e dependam das facilidades dos sistemas digitais, tenham um mínimo de conhecimento sobre os ataques e golpes mais comuns, para que saibam como se prevenir e evitar prejuízos catastróficos.

O objetivo deste trabalho é revisar e pontuar os crescentes golpes que ocorrem diariamente no ambiente cibernético, e reforçar conceitos pré-existentes de ameaças virtuais, dado que a constante evolução da tecnologia também implica na evolução dos métodos maliciosos e das ameaças.

METODOLOGIA

Na abordagem qualitativa os pesquisadores coletam evidências em várias fontes, tais como entrevistas, observações e documentos, não se confiando em uma única fonte. Finalmente, eles examinam todas as evidências, extraem sentido delas e as organizam em categorias ou temas (CRESWELL, 2010).

Essa pesquisa caracteriza-se como uma pesquisa qualitativa, quando o pesquisador se aprofunda no tema pesquisado. Em que foi também utilizada a pesquisa bibliográfica

para dar sustentação aos conceitos utilizados. E por fim, foi utilizada a revisão sistemática para levantar o atual momento sobre os ataques e defesas cibernéticos.

"A pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc., até meios de comunicação orais: rádio, gravações em fita magnética e audiovisuais: filmes e televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritos por alguma forma, querem publicadas, quer gravadas." (LAKATOS; MARCONI, 2003).

LEVANTAMENTO DOS DADOS

Aqui vamos relatar tentativas de ataques reais, bem como as dicas de como evitá-los. A revisão sistemática realizada buscou entender os ataques e as defesas possíveis, bem como a divulgação de orientações simples que os usuários e empresas podem e devem tomar para melhorar a segurança cibernética.

Primeiro caso: Criminosos se passam pelo governo federal através do envio de e-mails falsos. Em 2022, golpistas estavam utilizando um e-mail com domínio @gov.br para se passar pelo governo federal, com intuito de enganar brasileiros. A mensagem chega à vítima com um aviso sobre um suposto processo que tramita no STJ (Superior Tribunal de Justiça), entretanto, a ação é um golpe de phishing sofisticado e pode levar o usuário a baixar malware de acesso remoto. Conforme mostra a Figura 2, abaixo.

Figura 2– Falso e-mail se passando pelo STJ.

Fonte: https://tecnoblog.net/noticias/2022/02/02/exclusivo-e-mail-com-gov-br-e-usado-em-golpes/

Ao analisar as informações do remetente falso com o domínio "@gov.br", é possível observar que a mensagem partiu de um servidor privado da empresa Linode, conhecida por oferecer servidores de aluguel, ou seja, o criminoso utilizou um IP falso para mascarar um segundo IP que está associado ao arquivo presente no e-mail.Para impedir mensagens suspeitas e spoofing (prática de falsificação de e-mail). O Google usa dois sistemas de autenticação de remetente: o SPF (Sender Policy Framework) e o DKIM (DomainKeys Identified Mail). Cada e-mail enviado a um usuário do Gmail passa pelo processo de verificação feito por essas duas ferramentas.

Segundo caso: Criminosos usam técnicas de phishing para aplicar golpes no cadastro do pix. A popularidade do pagamento por Pix fez dele uma porta de entrada para aplicações de golpes e que podem aparecer inclusive durante a etapa de cadastro da chave. Essas ações começaram antes do lançamento do Pix, quando as instituições financeiras passaram a entrar em contato com os clientes para oferecer o pré-cadastro para esse meio de pagamento.

Os criminosos, então, transformaram isso em golpe. No geral, a tática usa o phishing em ações que imitam as campanhas legítimas de bancos e fintechs. São mensagens falsas que prometem facilitar o registro, mas que, na verdade, oferecem um link que leva a um site malicioso e que, muitas vezes, é bastante parecido com o original.

O objetivo dos fraudadores é coletar dados pessoais, como senhas e números de CPF e celular. Se o cliente fornece esses dados, os criminosos podem cometer golpes no futuro. Então, não se deve clicar em nada vindo de indivíduos ou organizações desconhecidos.

Outra forma de ação dos golpistas é fazer uma ligação telefônica para oferecer o cadastramento da chave Pix. O criminoso se passa por funcionário da instituição financeira e solicita dados pessoais e bancários. Lembre-se de que bancos e fintechs não fazem esse tipo de contato para solicitar informações pessoais.Para evitar ser vítima desse golpe, basta adotar algumas medidas simples:

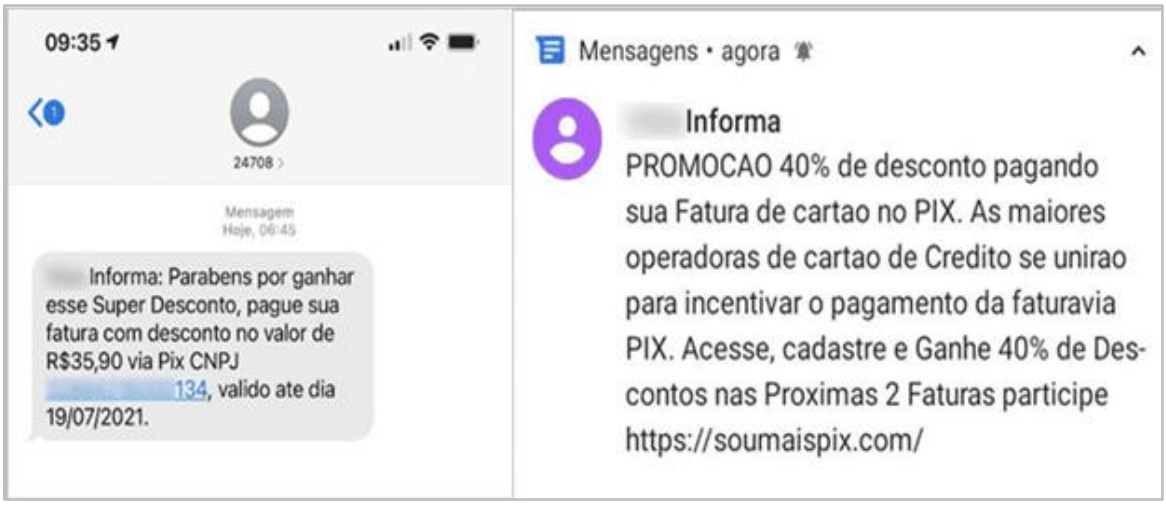
•Sempre confira se o endereço em que vai inserir qualquer dado é de fato da instituição financeira. A melhor medida é registrar as informações na plataforma específica que normalmente usa para ter acesso ao banco ou à fintech.

•Se receber mensagens que incentivam o cadastro da chave Pix e, para isso, oferecem um link, evite clicar nele. Ele pode ter um software para capturar informações pessoais.

•Os antivírus são capazes de bloquear domínios falsos muitas vezes antes mesmo de eles funcionarem. E há várias opções gratuitas desse tipo de software no mercado, como: Avast, Bitdefender, Pc protect, Total AV, entre outros.

Terceiro caso: Golpes do Pix por meio de SMS. As mensagens chegam à vítima por SMS e prometem desconto no pagamento de faturas de celular ou cartão de crédito utilizando Pix. Em um dos exemplos divulgados pela empresa de segurança (Kaspersky), a mensagem falsa afirmava que o consumidor poderia ter abatimento de R$ 35,90 na conta e em seguida, informava a chave Pix para a transferência do dinheiro, como mostra a Figura 3 abaixo.

Figura 3 - Golpes phishing por SMS.

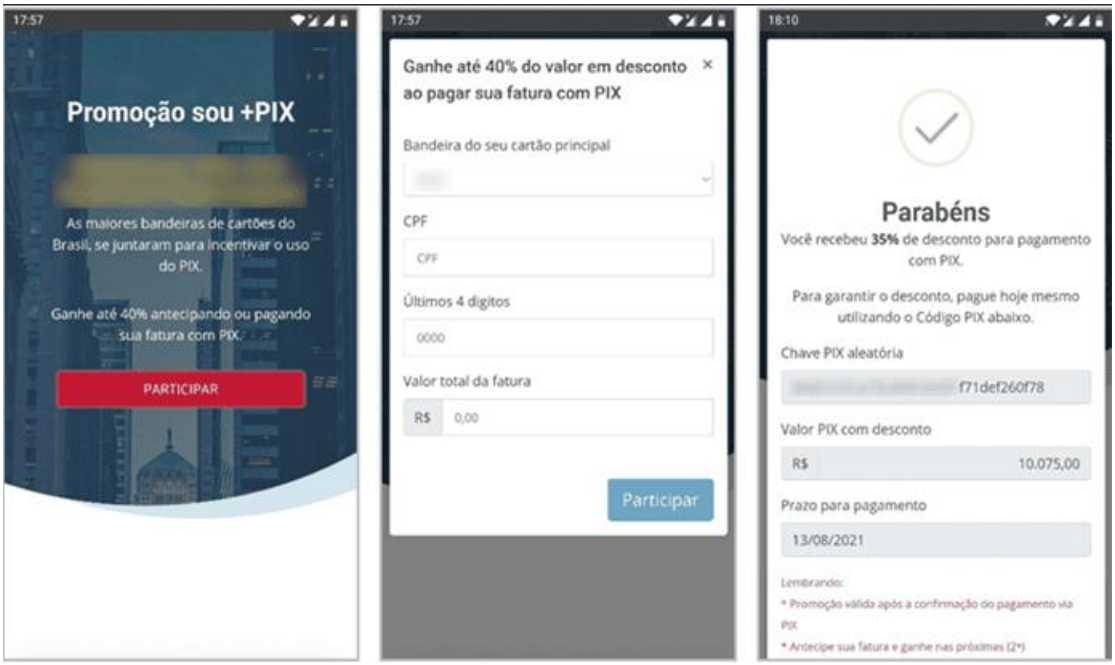


Fonte: https://www.kaspersky.com.br.

Um detalhe importante nesses golpes é o fato deles usarem números curtos para o envio dos SMSs falsos. São chamados de “short-code” e são canais que deveriam ser usados exclusivamente pelas operadoras e grandes empresas para realizar a comunicação com clientes, pois eles têm uma maior credibilidade e são usados geralmente para o envio de tokens ou códigos de confirmação, porém, a realidade é que eles estão sendo utilizados para aplicar golpes online.

Quarto caso: Usuários são induzidos a fazer transferência via Pix por meio de falsa promoção. Nesse caso foi enviada mensagem de um comunicado sobre a união entre as bandeiras de cartões para oferecer descontos de até 40% na fatura, a vítima é direcionada ao site falso www.soumaispix.compara gerar a conta com o valor reduzido. Para isso, ela precisa informar seu CPF, valor da fatura, bandeira e os quatro últimos números do cartão. Por fim, um novo valor falso para a fatura é gerado, e uma chave Pix é informada para transferência. Neste caso, além de perder dinheiro, a pessoa também acaba entregando dados pessoais de bandeja para os criminosos, como mostra a Figura 4 abaixo.

Figura 4 - Site prometendo falsa promoção do PIX.



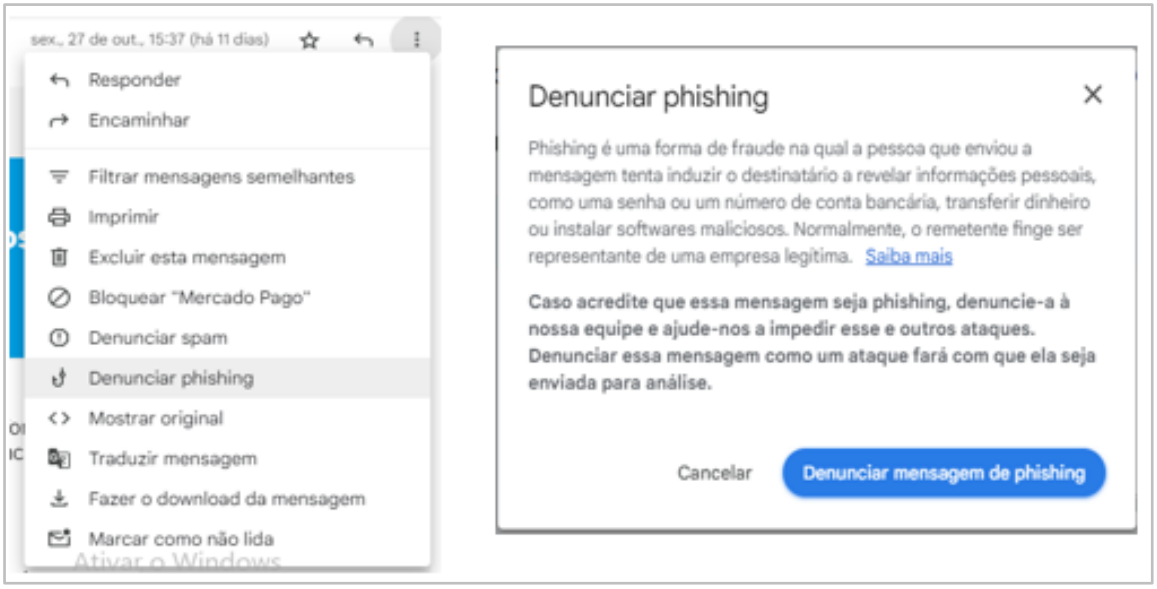
Fonte: https://www.kaspersky.com.br.

Para prevenir Phishing, analise cuidadosamente os tipos de e-mails que você abre e os links nos quais você clica. Preste muita atenção aos cabeçalhos de e-mail e não clique em nada que pareça suspeito, verifique os parâmetros "Responder para" e "Caminho de retorno". Eles precisam se conectar ao mesmo domínio apresentado no e-mail.

Denuncie mensagens que você julgar como estranho.

O Gmail possui uma ferramenta de denúncia na qual o usuário pode avisar para o google que uma determinada mensagem trata-se de suspeita de ataque phishing. Siga as instruções abaixo:Abra a mensagem que você quer denunciar; com a mensagem aberta, no canto superior direito, clique nos três pontos e depois na opção "Denunciar Phishing". Como mostra a Figura 5 abaixo.

Figura 5 – Como denunciar mensagens pishing no gmail?



Fonte: Elaborado pelo autor.

Aqui vão algumas dicas de como evitar golpes por pix?

1.Crie, no app do seu banco ou fintech, um limite diário para transferência via Pix. Alguns serviços só permitem essa configuração a cada período, então, é necessário que o usuário se programe;

2.Ao fazer transações via Pix, use somente o app ou site oficial do seu banco: desconfie de e-mails e links;

3.Confira sempre se o site do banco, da fintech ou das lojas que você está acessando e buscando algo para transacionar e/ou comprar é o correto;

4.Jamais clique em links, baixe ou execute arquivos que vem de e-mails suspeitos e não conhecidos: na dúvida, não clique;

5.Procure utilizar a Internet do seu aparelho telefônico quando estiver fora de casa e evite se conectar às redes públicas de wi-fi, como de shoppings, hotéis e restaurantes, especialmente se for se conectar às redes sociais ou ao aplicativo do seu banco;

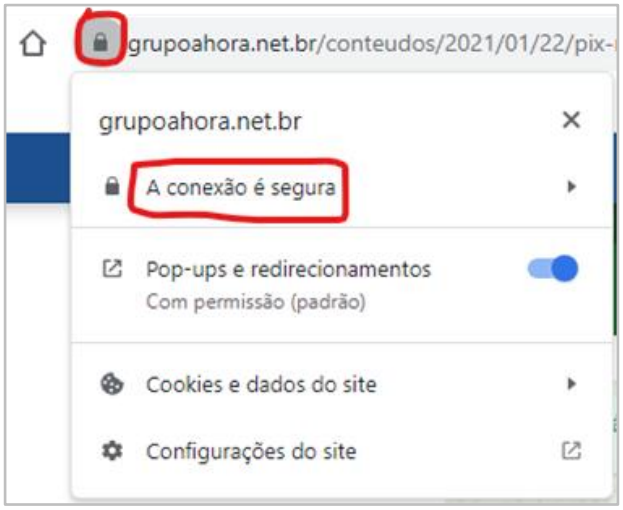
6.Não divulgue sua chave Pix na Internet ou para pessoas e empresas que você não tem relação de confiança. Caso opte for fazê-lo, informe a chave aleatória gerada pelo seu banco ao invés da atrelada ao CPF, CNPJ, e-mail ou telefone;

7.Ative a autenticação de duas etapas em todos os aplicativos que suportam essa função.

8.Quando for utilizar autenticação em dois fatores, dê preferência para aplicativos, como Google, Microsoft Authenticator e apps de banco. Após isso, a mensagem será denunciada como ataque phishing e será movida para caixa de spams.

9.Verifique se o site em que está acessando para realizar uma compra é seguro. Faça isso clicando no cadeado que fica na barra de endereço do navegador, conforme mostra a Figura 6 abaixo.

Figura 6 - Como verificar se um site é seguro?



Fonte: Elaborado pelo autor.

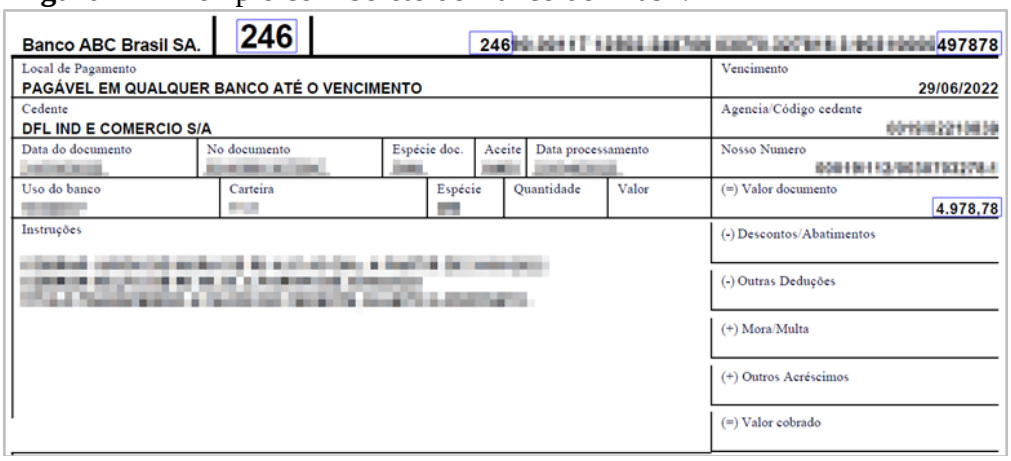
Quinto caso: Golpe do falso boleto. Trata-se da prática de estelionato, onde os criminosos levam a vítima a crer que está fazendo um pagamento correto. Como os boletos são um meio de pagamento muito comum no mercado, isso atrai a atenção dos fraudadores, especialmente quando encontram pessoas com pouco conhecimento do assunto ou até mesmo com tempo curto para fazer uma conferência mais apurada do boleto.

Como os criminosos agem: Os hackers enviam um boleto muito semelhante ao que o cliente costuma receber normalmente. O golpe não ocorre apenas online, com envio por e-mail, mas também com os boletos físicos.Apesar das semelhanças, o boleto falso terá o código de barras diferente do correto e desviará o pagamento para outra conta, alterando o código do credor.Como é um pouco difícil identificar o golpista, também existe uma dificuldade do cliente recuperar o valor pago indevidamente.Além disso, normalmente, o cliente só descobre após a empresa credora informá-lo do débito em aberto. Ou seja, muito tempo depois do pagamento ter sido efetuado.

Como se prevenir: Não clique em links ou e-mails suspeitos; Desconfie da origem do boleto ou cobrança; Verifique se os dados estão corretos; Tenha atenção ao código de

barras e ao valor. Confira o banco emissor da empresa em que você está realizando a compra. Os três primeiros números correspondem ao código do banco emissor e os números finais ao valor. Confira abaixo na Figura 7 abaixo.

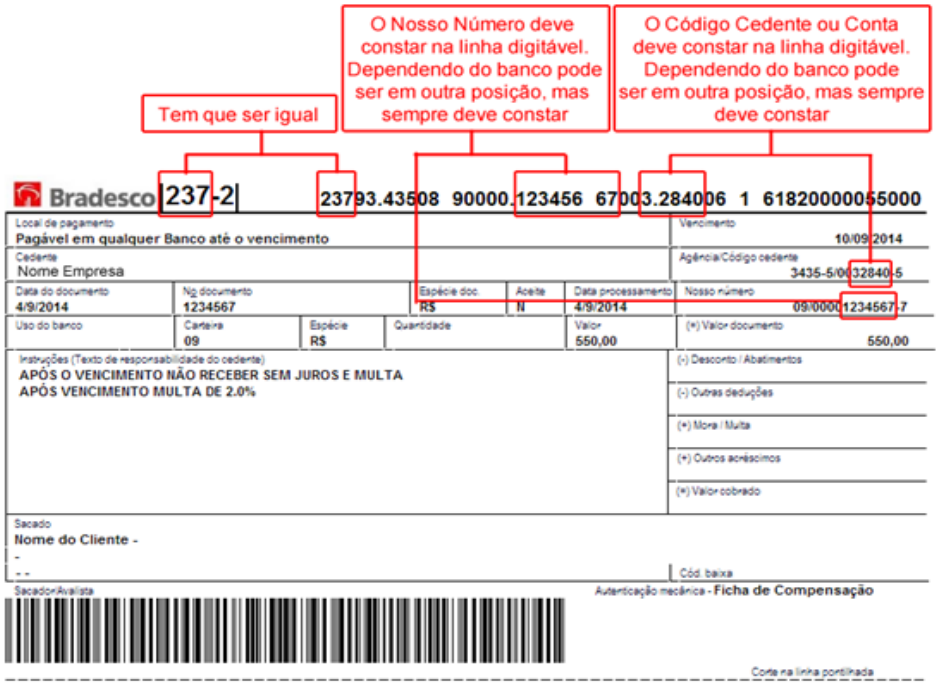
Figura 7 – Exemplo com boleto do Banco do Brasil.



Fonte: https://www.dfl.com.br/golpe-do-falso-boleto-saiba-como-se-proteger/

A Figura 8 abaixo, apresenta possíveis erros no documento. Informações divergentes ou erros ortográficos costumam ser frequentes em documentos e e-mails fraudados. Por isso sempre fique atento a esses sinais.

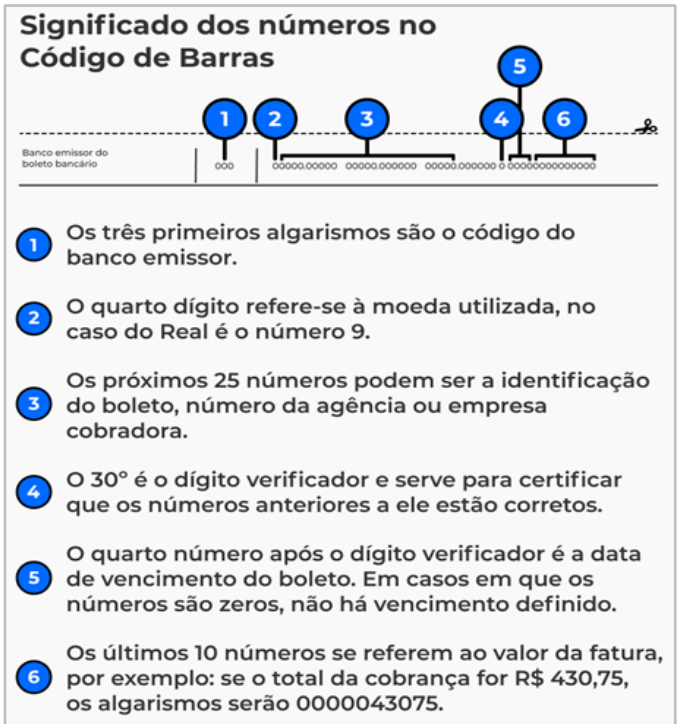
Figura 8 – Dicas para não cair no golpe do boleto.



Fonte: https://sisloc.com/blog/fique-atento-aos-golpe-do-boleto-falso/

Por último e não menos importante, verifique o código de barras do documento. Afinal, cada número que compõe o código de barras de um boleto bancário têm uma razão para estar ali, como mostra a Figura 9 abaixo.

Figura 9 - Significado dos números dos códigos de barras.



Fonte: https://www.cobrefacil.com.br/blog/boleto-verdadeiro.

Sexto caso: Golpe de tarefa online. De acordo com o site Uol no dia 18/10/2023, tomou-se ciência de um golpe em que se anunciava uma oportunidade de obter um pequeno retorno financeiro ao realizar pequenas tarefas em sites de vendas, sobre o pretexto de se prover um serviço de publicidade a vendedores.

Ao que se detalha ao longo da notícia, a vítima teria a opção de realizar tarefas gratuitas com pequeno retorno, ou tarefas pagas com um retorno superior, e a princípio as tarefas pagas de baixo valor teriam algum retorno, apenas para o golpista conquistar a confiança da vítima, e solicitar um valor exorbitante com a promessa de retorno exorbitante, e é aí obviamente que o golpe acontece. A relevância desse golpe para o contexto desta pesquisa, é pontuar uma nova perspectiva de retorno financeiro, que só é possível com a atual estrutura da internet, pois a princípio o golpe faz algum sentido, visto que o barateamento de serviços, sobretudo publicidade, é um dos pontos a ser alcançado com a constante evolução da tecnologia.

No mesmo site que descreve o golpe, há um relado de uma das vítimas que recebeu anúncios relatando que empresários já não estavam muito inclinados a gastar com publicidade, e que existia essa nova “Modalidade” de publicidade, que não demandava investimento, e tinha retorno garantido, a vítima relata:

> “Uma pessoa dizendo ser uma empresa de marketing digital me ligou, disse que eu poderia fazer uma renda extra apenas curtindo looks em uma plataforma e que eu não precisaria investir nada. Por não pedir nenhum dinheiro, eu acreditei que era verdade e aceitei a proposta. No primeiro dia fiz algumas tarefas e recebi R$ 36. Acreditando que era algo sério, fui seguindo com as tarefas e não desconfiei porque eles estavam depositando o meu pagamento. Mas no dia seguinte, eles informaram que tínhamos que fazer algumas

> tarefas pagas, mas que o valor retornaria para a gente corrigido". (Vítima do golpe).

Um detalhe muito comum em golpes de engenharia social é o investimento por parte da vítima, para obter alguma compensação posterior, e tem como alvo pessoas vulneráveis ou em situações complicadas que precisam de dinheiro.

Por mais que possa parecer legítimo, investimento prévio nunca é confiável, por mais que tenha sido redirecionado por um parente próximo, ou amigos, esse tipo de golpe precede a internet e já possui variações extremamente diversificadas, especialmente em forma de spam, e é tão comum que um dos golpes mais conhecidos de investimento prévio é de um "Principe nigeriano" em que consiste no pagamento de uma taxa para "liberar" uma fortuna que nunca existiu, um golpe tão clássico que é um ponto de referência quando se trata de golpes na internet.

Sétimo caso: Golpe da Biometria ou golpe da "cara falsa". De acordo com o site da Band, no dia 16/06/2023 é uma técnica que golpistas usam para criar contas em nome de pessoas aleatórias, utilizando imagens impressas de fotos das vítimas a fim de burlar o sistema de biometria facial, e uma vez que a conta é criada, os golpistas podem fazer empréstimos sem a ciência das vítimas, que só descobrem que sofreram o ataque quando recebem a fatura de cartão, como bem descreve o site: "Os bandidos abrem contas no nome das pessoas, com números de RG e celular falsos. Na hora de fazer o reconhecimento facial, os bandidos colocam uma foto impressa da pessoa no manequim e assim, conseguem burlar os aplicativos." (BAND,2023).

Por se tratar de um golpe que burla a segurança digital, inevitavelmente haverá melhorias nos sistemas de biometria a fim de que esse tipo de golpe seja impossível de replicar, portanto não é de se esperar ouvir muito falar nesse tipo específico, porém podemos perceber nesse caso, que sistemas de segurança extremamente sofisticados, nem sempre são implementados em todos os lugares, por motivos de custos e manutenção.

CONCLUSÕES

Nesta pesquisa levantamos alguns casos mais comuns de ataques com vítimas confirmadas, buscando propor ações de defesas dos usuários, mas com a constante evolução da tecnologia e inevitável evolução das ameaças, pode-se considerar que nenhum sistema será 100% seguro, logo é importante que ao menos os estudos de cibersegurança alcancem e preferencialmente ultrapasse o passo do avanço das ameaças, pois caso contrário as consequências serão catastróficas, dado que basta alguém mal-intencionado com acesso a sistemas restritos para causar um dano real.

Considerando a recente introdução de IA no desenvolvimento de malwares, pode-se esperar alguns surtos esporádicos ocasionados pelo deslize de medidas de segurança, portanto os danos não podem ser 100% evitados, mas podem ser minimizados com a conscientização das possíveis vítimas.

E a evolução não deve acontecer apenas na parte técnica dos estudos, pois o direcionamento e educação da população em geral poderá evitar o agravamento e desenvolvimento de situações e golpes exclusivamente sociais, considerando que casos individuais podem passar desapercebidos dado que as ameaças podem surgir de todas as formas possíveis.

Logo, podemos concluir que a luta contra as ameaças virtuais é uma peleja eterna, mas não é em vão, pois só é necessária uma única falha de segurança para que haja um colapso catastrófico de sistemas e serviços no qual dependemos diariamente.

REFERÊNCIAS BIBLIOGRÁFICAS

CRESWELL, J. W. Projeto de pesquisa: Métodos qualitativo, quantitativo e misto. 3ª ed. Porto Alegre: Ed. Artmed, 2010.

DIO.ME, Disponível em: https://www.dio.me/articles/entendendo-as-diferencas-entre-hackers-crackers-e-outros-termos-de-seguranca-cibernetica. Acesso em: 5 de Nov. de 2023.

FORTINET, Disponível em: https://www.fortinet.com/br/resources/cyberglossary/types-of-cyber-attacks. Acesso em: 2 de Nov. de 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 5. ed. São Paulo: Atlas, 2003.